AFFIDAVIT OF MICHAEL G. GERFIN

I, Michael G. Gerfin, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent (SA) with the Federal Bureau of Investigation ("FBI") since approximately August 2008. During this time, I have been assigned to numerous investigations involving complex computer crimes. I am currently assigned to the FBI Cleveland Division Cyber Crimes Squad and am responsible for investigations involving computer-related offenses. I have participated in the execution of numerous warrants involving the search and seizure of computers, computer equipment, software, and electronically stored information. In addition to my work experience, I have received extensive specialized training in the field of computer crime investigation from the FBI and others. In addition to my investigative experience, I possess degrees in Computer Science and Physics and have been involved in the field of information technology for over 20 years. My previous employment consisted of roles in computer network administration and software engineering, and I hold numerous professional certifications in the field of computer security.

2. I submit this affidavit in support of a criminal complaint charging JAMES E ROBINSON, date of birth 06/27/1985, with a violation of Title 18, United States Code, Section 1030(a)(5)(A), that is, knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer.

3. The statements in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement officers, victims

and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

TECHNICAL TERMS

4. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

d. Distributed denial of service (DDoS) attack: A DDoS attack is an attack against a specific server or servers on the Internet that attempts to illegitimately utilize a collection of computer systems in an effort to bring down the targeted server(s) by sending an excessive amount of malicious network traffic over the Internet to a host. This can be accomplished in several ways. In most cases, an attacker will utilize a large collection of systems on the Internet, called a botnet, which can be controlled remotely and instructed to attack a targeted system. In other instances, attackers can utilize a for-hire service that provides the necessary infrastructure to launch attacks. The end result is the targeted system becomes overwhelmed with network traffic causing it to crash, or ties up resources which ultimately denies legitimate users from being able to access the server. Even a single system is capable of executing a denial of service (DoS) attack against an Internet accessible server, if the offending computer is able to generate enough traffic to overwhelm the targeted site.

PROBABLE CAUSE

5. On or about August 1, 2017, personnel from Interactive Media Group, also known as EyeMG, a group that manages websites and Internet services, began receiving email alerts concerning network traffic to their servers. Upon investigating the alerts, it was discovered that servers hosting websites belonging to the City of Akron, Ohio, located in the Northern District of Ohio, were victims of an active DDoS attack. It was eventually discovered that the attack was distributed, meaning that malicious traffic originated from a large collection of IP addresses. Two website domains appeared to be the target of the attacks, namely *akronohio.gov* and *akroncops.org*.

6. The DDoS attack ultimately overwhelmed the websites with network traffic and rendered them unavailable to users. Information technology personnel from EyeMG attempted to move the systems to a disaster recovery location utilizing different IP addresses, but the attacker was able to shift the target, and continued the attack for several days. The attack continued through approximately August 5, 2017, and the above websites were unavailable to legitimate users for a portion of the time during the attack.

7. In my training and experience, it is common for hacktivists[1] to post the results of their attacks to social media websites. This allows the hacktivist to advertise his or her cause, to gain personal notoriety and alert other hackers that the attacks and techniques employed by the hacktivist were successful.

8. On or about August 1, 2017, at approximately 9:45 p.m., a tweet by moniker @AkronPhoenix420 on the social media website Twitter took credit for targeting the Akron, Ohio, website located at http://www.akronohio.gov. The tweet included a link to a YouTube video at youtube.com/watch?v=BW12vynlv0c, the hastags #Anonymous, #Phoenix420, and #TangoDown[2], along with the text 'akronohio.gov' and '208.79.157.50'. The victim subsequently confirmed this IP address was under attack during that time period. Another tweet issued from the same moniker showing a screenshot of website https://check-host.net demonstrating that the website *akronohio.gov* was not accessible. The screenshot had a displayed date and time of August 1, 2017, at 8:11 p.m.

[1] A "hacktivist" is someone who maliciously harms computers, servers and/or website domains to gain attention for a political or socially motivated purpose.

[2]. A hashtag allows users of social media sites to associate posts with a specific topic or group. In my training and experience, the hashtag #TangoDown is often used by a hacker to announce that an attack facilitated over the Internet was successful.

9. The Twitter account @AkronPhoenix420 issued multiple tweets with references to the hacker group Anonymous[3], along with specific tweets referencing the DDoS attack against the City of Akron, Ohio, websites. This included a tweet on August 1, 2017, which referenced website domain *akronohio.gov*, IP address 208.79.157.50, and included the hashtags #Anonymous, #Phoenix420, and #TangoDown.

10. In addition to the above, the described tweet included a link to a YouTube video titled "OpEXPOSED AKRON PD". This video was posted by a user employing the moniker "Akron Phoenix420" and included a recorded video message showing a static image of an individual in a Guy Fawkes mask making statements including, "it's time we teach the law a lesson," "Akron PD abuses the law," and "this week the city of Akron experienced system failures on multiple domains including their emergency TCP ports."

11. In addition to the tweets announcing the City of Akron, Ohio, DDoS attacks, the @AkronPhoenix420 Twitter account also revealed the use of several tools capable of enabling a DDoS attack, to include the Low Orbit Ion Cannon (LOIC).[4]

12. It is common for hackers targeting computer systems over the Internet to conduct a basic scan or probe of a system when preparing for a larger attack. This can include port

[3] "Anonymous", as it pertains to the hacker community, is a group of international hacktivists who are generally self-proclaimed members. They tend to show support for social and political movements through online 'operations' that involve attacking specific sites on the Internet, publicly outing individuals or groups by posting derogatory information, and developing messaging and propaganda to further their agenda. Members of Anonymous often reuse similar imagery or disguises to show their affiliation in online videos or images. One such example is the use of a Guy Fawkes mask. The Guy Fawkes mask, which portrays a white male face with a thin black moustache and beard, has been frequently used by members of Anonymous to hide their faces during protests or creation of propaganda over the past 10 years.

[4] The Low Orbit Ion Cannon (LOIC) is an open-source network stress testing and denial-of-service attack application. It has been used within the hacker and computer penetration testing community for a number of years to initiate denial of service attacks against servers on the Internet.

scanning and tool testing to determine if the target is susceptible to the attack. Information Security personnel for EyeMG which hosts several of the City of Akron, Ohio, websites conducted log analysis and identified several IP addresses which were associated with scanning and/or reconnaissance activity prior to the attack. The probing traffic from these IP addresses included references to 'Anonymous' and 'LOIC'.

13. An example of such traffic occurred on multiple occasions between July 06, 2017, and July 30, 2017, originating from IP address 24.93.205.42. Legal process was served to Charter Communications regarding this address. Charter Communications responded that this IP address was associated with a residential Internet connection registered to JAMES E. ROBINSON and was assigned IP address 24.93.205.42 from July 5, 2017, at 11:18:10 p.m. EDT through August 29, 2017, at 9:17:04 a.m. EDT. The contact information for the account included telephone number 989-264-5985.

14. Legal process was issued to Verizon Wireless for information relating to the subscriber of telephone number 989-264-5985. Verizon Wireless responded that this number was subscribed to by JAMES E. ROBINSON.

15. Legal process served to Twitter resulted in the production of IP connection records for Twitter account @AkronPhoenix420 which contained an entry indicating a *last_login_ip* of 174.232.3.79 on January 3, 2018, at 10:30:12 GMT. IP assignment logs for the Verizon Wireless account with telephone number 989-264-5985 contained multiple entries indicating IP address 174.232.3.79 was assigned to this account between January 2, 2018, at 23:31 GMT and January 3, 2018, at 14:30 GMT. The above records demonstrate that the user of Twitter account @AkronPhoenix420 used a Verizon cellular phone subscribed to by JAMES E. ROBINSON.

16. Between approximately February 15, 2018, and February 19, 2018, the Verizon Wireless account associated with telephone number 989-264-5985 was suspended due to lack of payment. Further legal process regarding multiple numbers which connected to this account enabled your affiant to identify telephone number 330-815-9821 as a potential new number for JAMES E. ROBINSON.

17. Legal process to Verizon Wireless requesting subscriber information for telephone number 330-815-9821 identified the subscriber as JAMES E. ROBINSON.

18. DDoS attacks have also been made against website domains and servers hosted by the State of Ohio Department of Public Safety, the National Institute of Health, the Defense Information Security Agency, the Department of Defense, the Department of the Treasury, and dozens of other targets around the world. These attacks bear many similar characteristics such as the method of attack and the targeted domains were specifically mentioned by twitter moniker @AkronPhoenix420. Based on the evidence gathered in this investigation and my training and experience, I believe these attacks were committed by the same individual or group.

19. JAMES E. ROBINSON did not have permission to conduct DDoS attacks against any of the website domains named herein and there was no legitimate purpose for directing large amounts of network traffic towards those domains. The attacks caused several of the website domains named herein to become inoperable for a period of time and negatively affected other computer systems without the owners' permission.

20. Multiple DDoS attacks have been claimed by Twitter moniker AkronPhoenix420, including many since January 1, 2018. On April 25, 2018, AkronPhoenix420 issued multiple tweets taking credit for an attack against website domain *akronohio.gov*. Law enforcement personnel from the city of Akron, Ohio, confirm that a DDoS attack took place on that day.

21. On April 26, 2018, after public release of news that authorities took down a DDoS provider accessible at Internet domain *webstresser.org*, @AkronPhoenix420 posted the following information in a tweet: "Okay guys quick update the ships getting thick after the last attack on NATO and Akron Ohio. Gov another stressor that I used in all my attacks that I've ever done has been wiped out the first one was quiz stress after attacking NATO and taking".

22. An additional tweet on April 26, 2018, included the following: "The second stressor was web stress. Org both of these structures were very powerful web stress had only use a layer for no layer 7 and could wipe out websites left and right as well as servers".

23. Another tweet on April 26, 2018, included the following: "I have always used an anonymous Alias and an anonymous email address through vpns masking and high-security to where I could not be tracked physically and on the Move throw away phones".

24. On May 9, 2018, the Honorable Magistrate Judge Kathleen Burke authorized a search warrant for the residence of JAMES E. ROBINSON located at 1268 Edison Avenue, Akron, Ohio, 44301.

25. On May 10, 2018, agents executed the search warrant. In the residence, agents located a Guy Fawkes mask and a cellular telephone with a distinctly cracked screen. A photograph of what appears to be the same phone was previously posted by Twitter account @AkronPhoenix420 on April 26, 2018, where the screen of the phone displayed the LOIC for Android application with a target URL of 'akronohio.gov'. JAMES E. ROBINSON was the only individual in the residence. ROBINSON was told that he was free to leave but indicated that he wanted to cooperate with authorities in any way he could. ROBINSON stated that he had used webstresser.org to conduct DDoS attacks against multiple sites on the Internet, include Department of Defense, Defense Information Systems Agency, and the City of Akron, Ohio.

ROBINSON advised there were other attacks, but he did not recall all of them. ROBINSON further stated that he was the author of tweets, photographs and videos posted by online, and that he used the moniker Phoenix420.

CONCLUSION

26. Based on the foregoing, there is probable cause to believe that between on or about July 6, 2017, and on or about May 10, 2018, the defendant, JAMES E. ROBINSON did knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage without authorization to a protected computer, in violation of 18 U.S.C. Section 1030(a)(5)(A).

Respectfully submitted,

Michael G. Gerfin
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on May 10, 2018.

UNITED STATES MAGISTRATE JUDGE